Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Установка, обновление и удаление

RU.88338853.501410.007 91 2

Почтовый адрес:	**127018, г. Москва, ул. Сущёвский Вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений

AD	Active Directory
IIS	Internet Information Server
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
OID	Object Identifier
SID	Security Identifier
SP	Service Pack
USB	Universal Serial Bus
XML	Extensible Markup Language
БД	База данных
ИС	Информационная система
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ОСР	Общедоступный сетевой ресурс
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности
СНК	Серийный номер клиента
СНС	Серийный номер сервера безопасности
СНУ	Серийный номер средств управления
СУБД	Система управления базами данных
ЦУ	Централизованное управление
ЭИ	Электронный идентификатор

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 6" RU.88338853.501410.007 (далее — система Secret Net 6, система защиты). В нем содержатся сведения, необходимые администраторам для установки системы защиты, ее обновления, исправления и удаления.

Перед изучением данного руководства необходимо ознакомиться с документом [1].

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Глава 1
Установка

Структура системы Secret Net 6 является модульной. Подробные сведения об архитектуре системы Secret Net 6 содержатся в документе [1].

Система Secret Net 6 состоит из следующих отдельных программных средств:

1. Компонент "Secret Net 6" (далее — клиент).
2. Компонент "Модификатор схемы Active Directory" (далее — модификатор AD). Используется только в сетевом режиме функционирования. Применяется однократно перед установкой других компонентов системы.
3. Компонент "Secret Net 6 — Сервер безопасности" (далее — сервер безопасности или СБ). Используется только в сетевом режиме функционирования.
4. Компонент "Secret Net 6 — Средства управления" (далее — средства управления). Используется только в сетевом режиме функционирования.

Требования к аппаратному и программному обеспечению

Клиент

Компонент "Secret Net 6" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС):

- Windows 7;
- Windows Server 2008 SP2/Server 2008 R2;
- Windows Vista SP2;
- Windows Server 2003 SP2/Server 2003 R2 SP2;
- Windows XP Professional SP3/XP Professional x64 Edition SP2;
- Windows 2000 SP4 Update Rollup 1.

На компьютере должен быть установлен обозреватель Internet Explorer версии 5.00.2314.1003 или выше. Программа установки компонента автоматически проверяет и при необходимости устанавливает следующие обновления:

- на компьютере с 32-разрядной версией ОС: Update Rollup (только для Windows 2000), Windows Installer 3.1, C/C++ Runtime для платформы x86;
- на компьютере с 64-разрядной версией ОС: C/C++ Runtime для платформ x86 и x64.

После установки обновлений может потребоваться перезагрузка компьютера.

Минимальные и рекомендуемые аппаратные требования, предъявляемые к компьютеру, аналогичны системным требованиям для соответствующей ОС.

Системный каталог ОС Windows %SystemRoot% должен располагаться на томе с файловой системой NTFS или NTFS5.

Если на компьютере предполагается использовать персональные идентификаторы eToken, iKey или Rutoken, рекомендуется до начала установки Secret Net 6 установить соответствующее программное обеспечение для работы с USB-ключами. Если на компьютере предполагается использовать другие устройства аппаратной поддержки (Программно-аппаратный комплекс "Соболь", Secret Net Card и др.), их следует устанавливать в соответствии с рекомендациями документа [8].

Компоненты для сетевого режима функционирования

В сетевом режиме функционирования системы Secret Net 6 помимо компонентов самой системы защиты в домене должны быть установлены компоненты СУБД Oracle. Также для выполнения задач администрирования требуются следующие стандартные средства системы Microsoft Windows Server 2000/2003/2008:

- средства централизованного управления Microsoft Administration Tools Pack (Admin Pack) — устанавливаются на компьютеры администраторов, ответственных за централизованное управление системой защиты;
- инструментальные средства Microsoft "Support\Tools" (Support Tools) — устанавливаются на контроллере домена.

Модификатор AD

Для применения компонента "Модификатор схемы Active Directory" компьютер, с которого выполняется модификация схемы, должен быть подключен к сети для установки соединения с контроллером домена. Других специальных требований к программной и аппаратной конфигурации компьютера не предъявляется.

Сервер безопасности

Компонент "Secret Net 6 — Сервер безопасности" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС):

- Windows Server 2008 SP2/Server 2008 R2;
- Windows Server 2003 SP2/Server 2003 R2 SP2;
- Windows 2000 Server SP4 Update Rollup 1.

Для работы сервера безопасности должна быть создана база данных на сервере баз данных Oracle версии Oracle9i 9.2.0.4e или выше. Возможны следующие варианты установки программного обеспечения сервера безопасности и Oracle:

- 1 вариант — ПО сервера безопасности и серверная часть Oracle устанавливаются на разных компьютерах (на компьютере с ПО СБ установлена только клиентская часть Oracle);
- 2 вариант — ПО сервера безопасности и ПО Oracle (серверная и клиентская части) устанавливаются на одном компьютере.

Для установки сервера безопасности на компьютере должно быть установлено следующее ПО:

- IIS 6.0 (на компьютере с ОС Windows Server 2003);
- IIS 5.0 (на компьютере с ОС Windows 2000 Server);
- MsXml 4.0 SP2 (на компьютере с ОС Windows 2000 Server);
- ПО Oracle.

Установка и настройка IIS на компьютере с ОС Windows Server 2008 осуществляется автоматически программой установки сервера безопасности.

Программа установки компонента автоматически проверяет и при необходимости устанавливает следующие обновления:

- на компьютере с 32-разрядной версией ОС: Update Rollup (только для Windows 2000), Windows Installer 3.1, C/C++ Runtime для платформы x86;
- на компьютере с 64-разрядной версией ОС: C/C++ Runtime для платформ x86 и x64.

После установки обновлений может потребоваться перезагрузка компьютера.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Оперативная память	512 Мбайт[1)]	1 Гбайт[2)]
Жесткий диск (свободное пространство)	10 Гбайт	50 Гбайт
Высокопроизводительный жесткий диск (свободное пространство)[3)]	100 Гбайт	100 Гбайт
[1)] 1 Гбайт для Windows 2003/2008. [2)] 2 Гбайт для Windows 2003/2008. [3)] Для 2-го варианта объем свободного пространства задан для случая, когда СУБД работает с сервером безопасности, имеющим 500 подчиненных компьютеров.		

Требования к программной и аппаратной конфигурации компьютера с отдельно установленным ПО серверной части Oracle аналогичны системным требованиям для соответствующей версии Oracle.

Средства управления

Компонент "Secret Net 6 — Средства управления" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС):

- Windows 7;
- Windows Server 2008 SP2/Server 2008 R2;
- Windows Vista SP2;
- Windows Server 2003 SP2/Server 2003 R2 SP2;
- Windows XP Professional SP3/XP Professional x64 Edition SP2;
- Windows 2000 SP4 Update Rollup 1.

Для установки средств управления на компьютере должно быть установлено следующее ПО:

- Internet Explorer версии 5.00.2314.1003 или выше;
- MsXml 4.0 SP2 (на компьютере с ОС Windows 2000);
- компонент "Secret Net 6" в сетевом режиме функционирования.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Оперативная память	256 Мбайт[1)]	512 Мбайт[2)]
Жесткий диск (свободное пространство)	500 Мбайт	2 Гбайт
[1)] 1 Гбайт для Windows 2003/Vista/2008/7. [2)] 2 Гбайт для Windows 2003/Vista/2008/7.		

Серийные номера, их назначение и особенности

Для эксплуатации системы Secret Net 6 необходимо приобрести и зарегистрировать лицензии на использование компонентов. Лицензии регистрируются посредством ввода серийных номеров при установке компонентов или в процессе эксплуатации системы.

Регистрация соответствующего серийного номера является обязательным условием при установке следующих компонентов:

- компонент "Secret Net 6";
- компонент "Secret Net 6 — Сервер безопасности".

Для лицензирования применяются следующие типы серийных номеров:

- серийный номер клиента (СНК);
- серийный номер сервера безопасности (СНС);
- серийный номер средств управления (СНУ).

Серийный номер клиента

СНК содержит лицензию на использование компонента "Secret Net 6" определенной версии (версий). Лицензия может быть бессрочной или с ограниченным сроком действия (демонстрационная). При регистрации серийного номера с демонстрационной лицензией возможность использования компонента ограничивается сроком действия лицензии. По окончании этого срока защитные функции принудительно отключаются и пользователю выводятся соответствующие сообщения. Для дальнейшего использования компонента необходимо ввести серийный номер с бессрочной лицензией (описание процедуры ввода серийного номера см. в документах [3], [7]).

СНК определяет разрешенный режим функционирования компонента — сетевой или автономный. Для сетевого режима функционирования дополнительно устанавливается ограничение на количество клиентов, для которых можно использовать данный серийный номер.

Лицензия может устанавливать ограничение на количество доступных защитных функций компонента. Набор защитных функций определяется вариантом применения системы Secret Net 6.

Серийный номер сервера безопасности

СНС содержит лицензию на использование компонента "Secret Net 6 — Сервер безопасности" определенной версии (версий). Лицензия может быть бессрочной или с ограниченным сроком действия (демонстрационная). При регистрации серийного номера с демонстрационной лицензией возможность использования компонента ограничивается сроком действия лицензии. По окончании этого срока сервер не допускает подключение рабочих станций, а при подключении программ управления выводятся предупреждающие сообщения. Для дальнейшего использования компонента необходимо ввести серийный номер с бессрочной лицензией (описание процедуры ввода серийного номера см. в документе [7]).

Лицензия дополнительно определяет ограничение на максимальное количество клиентов, подчиняемых серверу безопасности с данным серийным номером.

Серийный номер программ управления

СНУ содержит лицензию на использование дополнительных подключений компонентов "Secret Net 6 — Средства управления" к серверу безопасности (без СНУ допускается одно подключение). В лицензии заданы ограничения на количество дополнительных компьютеров, с которых возможно одновременное подключение программ "Монитор" и/или "Журналы" к СБ.

Примечание. При поочередном использовании на разных компьютерах программ "Монитор" и/или "Журналы" СНУ не требуется.

Версия ПО средств управления, заданная в СНУ, должна совпадать с версией ПО СБ в СНС — в противном случае СНУ считается недействительным.

Установочный компакт-диск системы

Программное обеспечение и эксплуатационная документация системы Secret Net 6 поставляются на установочном компакт-диске. Общая структура каталогов диска представлена в следующей таблице:

Каталог	Содержимое
\Setup\AD\	Программа модификации схемы Active Directory
\Setup\Client\	Дистрибутивы клиента
\Setup\OM\	Дистрибутив средств оперативного управления
\Setup\Server\	Дистрибутив сервера безопасности
\Setup\SnTmCard\	Файлы установки драйвера средства аппаратной поддержки
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты

Программа автозапуска

При вставке установочного диска в привод для чтения дисков CD-ROM происходит автоматический запуск программы (далее — программа автозапуска), которая позволяет выполнять следующие действия:

- запускать программы установки компонентов системы Secret Net 6;
- открывать в отдельных окнах каталоги диска.

Если на компьютере отключена функция автозапуска компакт-дисков, автоматический запуск программы не выполняется. В этом случае для работы с программой автозапуска запустите файл SnAutoRun.exe, расположенный в корневом каталоге компакт-диска.

В окне программы автозапуска представлены команды для выполнения действий. Назначение команд описано в следующей таблице:

Команда	Назначение
Модификатор схемы AD	Запускает программу модификации схемы Active Directory
Клиентское ПО	Запускает программу установки клиента
Сервер безопасности	Запускает программу установки сервера безопасности
Средства управления	Запускает программу установки средств управления
Дополнительное ПО	Открывает в отдельном окне каталог \Tools\
Документация	Открывает в отдельном окне каталог \Documentation\
Обзор диска	Открывает в отдельном окне корневой каталог диска
Выход	Завершает работу программы

Для выполнения нужного действия активируйте соответствующую команду. Некоторые команды запуска могут быть заблокированы из-за невозможности установки компонентов или если установка не требуется. Для просмотра сведений о причине блокировки наведите указатель на команду — через 1–2 секунды на экране появится всплывающее сообщение.

Установка клиента в автономном режиме функционирования

Установка клиента в автономном режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для установки клиента в автономном режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. выше) и запустите установку с помощью команды "Клиентское ПО".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните соответствующее действие:

   - если установку необходимо выполнить на компьютер с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
   - если установку необходимо выполнить на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий. Перед началом процедуры установки на экране появится диалог для выбора режима работы компонента.

2. Установите отметку в поле "Автономный режим" и нажмите кнопку "Далее >".

   По окончании подготовительных действий на экран будет выведен диалог приветствия программы установки.

3. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер".

5. Введите серийный номер продукта — системы Secret Net 6.

   Пояснение. Без ввода серийного номера установка невозможна.

6. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Папка назначения".

7. Оставьте заданную по умолчанию папку установки программного обеспечения или укажите другую папку назначения и нажмите кнопку "Далее >".

   На экране появится диалог "Учетная информация компьютера".

8. Заполните поля диалога учетными данными и нажмите кнопку "Далее >".

   При установке на ОС Windows 2000/XP на экране появится диалог "Дополнительные параметры". Если выполняется установка на другой ОС, на экране появится диалог "Готова к установке программы" — в этом случае пропустите действия **9–10**.

9. При установке на ОС Windows 2000/XP определите необходимость замены установленных по умолчанию прав доступа пользователей к основным ресурсам компьютера. Если требуется заменить права доступа пользователей, оставьте отмеченным поле "выполнить расстановку прав доступа на файлы, каталоги и ключи реестра".

   Пояснения.

   - Замена прав доступа усиливает защищенность операционной системы, однако выполнять ее рекомендуется только в тех случаях, когда после установки ОС администратор не осуществлял специальную расстановку прав доступа. Перечень устанавливаемых прав доступа для соответствующих ОС см. в Приложении на стр. 35 и 37.
   - Права доступа на каталог установки системы Secret Net 6 устанавливаются для любой ОС в обязательном порядке независимо от выбранного режима расстановки прав. Перечень устанавливаемых прав доступа к каталогу установки см. в Приложении на стр. 39.

10. Для продолжения установки нажмите кнопку "Далее >".

    На экране появится диалог "Готова к установке программы".

11. Нажмите кнопку "Установить".

    Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

    В процессе установки ПО на экране могут появляться различные запросы системы. В частности, запросы на выбор нужных действий выводятся в следующих случаях:

    - При установке на ОС Windows Vista и выше перед добавлением в систему драйвера средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card появляется запрос на установку драйвера. Если на данном компьютере такое изделие использоваться не будет, можно отказаться от установки драйвера. При подтверждении установки драйвер регистрируется в системе в качестве самостоятельного компонента (при установке на ОС Windows 2000/XP/2003 драйвер регистрируется по умолчанию). Сведения о средствах аппаратной поддержки см. в документе [8].
    - Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net 6 может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net 6.

    Перед завершением установки требуется выполнить окончательную настройку ПО. Действия для окончательной настройки выполняются в диалоговом окне "Управление Secret Net 6", процедуры работы с которым описаны в документах [3] и [8]. На этапе установки достаточно закрыть диалоговое окно, не внося никаких изменений.

12. После окончательной настройки перезагрузите компьютер.

Внимание! Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Порядок установки для сетевого режима функционирования

Установка системы Secret Net 6 в сетевом режиме функционирования осуществляется в следующей последовательности:

1. Включите все контроллеры домена.
2. Установите на контроллере домена инструментарий Windows Support Tools из состава дистрибутива ОС.
3. Выполните модификацию AD и дождитесь репликации схемы AD на все контроллеры домена.
4. На компьютерах, которые будут использоваться в качестве серверов безопасности, установите:
   - ПО сервера безопасности;
   - ПО клиента.
5. На рабочих местах администраторов Secret Net 6 установите:
   - средство Microsoft Administration Tools Pack из состава дистрибутива ОС Windows серверных платформ;
   - ПО клиента;
   - средства управления.
6. Установите ПО клиента системы Secret Net 6 на серверы и контроллеры домена, затем на компьютеры сотрудников.

Совет. При большом количестве компьютеров целесообразно применить автоматическую установку ПО клиента. Сведения о настройке автоматической установки см. в Приложении на стр. 40.

Модификация схемы Active Directory

Модификацию схемы AD должен выполнять пользователь, входящий в группу администраторов "Schema Admins" и имеющий право записи в AD. Модификацию AD можно проводить с любого компьютера домена (леса).

Подробные сведения об изменениях в AD при модификации схемы см. в Приложении на стр. 29.

Для модификации схемы AD

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и активируйте команду "Модификатор схемы AD" (или запустите с установочного компакт-диска файл \Setup\AD\SnADMS.exe).

   На экране появится диалог "Модификатор схемы Active Directory", модификатор AD автоматически найдет контроллер домена, являющийся мастером схемы AD, и на фоне диалога появится сообщение: "Поиск мастера схемы Active Directory успешно завершен".
2. Нажмите кнопку "OK".

   На экране появится диалог "Параметры модификации схемы Active Directory".
3. Заполните поля "Пользователь" и "Пароль" данными учетной записи пользователя, входящего в группу "Schema Admins".

   Совет. Если вход на компьютер выполнен под учетной записью пользователя, входящего в группу "Schema Admins", поля "Пользователь" и "Пароль" можно не заполнять.
4. Для запуска процесса модификации AD нажмите кнопку "Применить".

   На экране появится запрос для подтверждения операции.
5. Для начала процесса модификации нажмите кнопку "Да".

   Начнется процесс модификации AD, по окончании которого на экране появится сообщение: "Модификация схемы Active Directory успешно завершена".
6. Для выхода из программы нажмите кнопку "Закрыть".

Установка сервера безопасности

Установка сервера безопасности выполняется пользователем, входящим в группу администраторов домена.

Перед установкой сервера безопасности необходимо установить компоненты СУБД Oracle (сведения о вариантах установки ПО Oracle см. на стр. 7).

Для установки сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите установку с помощью команды "Сервер безопасности".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного компакт-диска файл \Setup\Server\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог принятия лицензионного соглашения.

3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".

4. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   На экране появится диалог "Серийные номера".

5. Введите серийные номера сервера безопасности (СНС), клиента (СНК) и средств управления (СНУ).

   Пояснения.

   - Без ввода СНС установка сервера безопасности невозможна.
   - СНК и СНУ на установку сервера безопасности не влияют — их можно добавить позже в программе "Консоль управления" (см. документ [7]). При установке сервера безопасности можно зарегистрировать один или несколько СНК, что позволит в дальнейшем автоматически регистрировать эти номера на клиентах, подчиняемых данному СБ. СНУ вводится, если к данному серверу безопасности планируется подключение программ управления с нескольких рабочих мест одновременно.

6. Нажмите кнопку "Далее >".

   На экране появится диалог "Папка назначения".

7. Оставьте заданную по умолчанию папку установки сервера безопасности или укажите другую папку назначения и нажмите кнопку "Далее >".

   На экране появится диалог "Настройки СУБД".

8. Выполните следующие действия:

   - Укажите параметры соединения сервера безопасности с тем экземпляром БД, который предназначен для работы с устанавливаемым сервером безопасности:
     - в поле "Имя БД" — укажите строку соединения с экземпляром БД в виде: *<имя_или_IP-адрес_сервера_Oracle>*/*<имя_экземпляра_БД>*

       Примечание. Имя или IP-адрес сервера Oracle можно не указывать, если серверная часть Oracle установлена на этом же компьютере.

     - в поля "Имя" и "Пароль" — данные учетной записи администратора БД или системное имя SYSTEM и его пароль, заданный при установке компонентов Oracle.

- Оставьте заданный по умолчанию или укажите другой каталог для размещения резервных копий журналов Secret Net 6.
- Нажмите кнопку "Далее >".

При успешном соединении с БД установка сервера безопасности будет продолжена и на экране появится диалог "Настройки ISAPI-расширения".

9. Оставьте заданный по умолчанию или укажите другой каталог для хранения временных файлов и нажмите кнопку "Далее >".

На экране появится диалог "Подчинение сервера".

Примечание. Диалог не появится, если устанавливается первый сервер безопасности. В этом случае пропустите действие 10.

10. Выполните следующие действия:

- Определите подчиненность устанавливаемого сервера безопасности:
  - если не требуется подчинять сервер безопасности другим серверам — выберите пункт "не подчинять этот сервер другому серверу";
  - если требуется установить подчиненность устанавливаемого сервера безопасности — выберите пункт "подчинить этот сервер другому серверу и настроить параметры подключения" и из раскрывающихся списков выберите имя хоста родительского сервера и скоростные параметры вашей ЛВС.

  Пояснение. В списке поля "Скорость подключения" содержатся названия шаблонов сетевых настроек устанавливаемого сервера безопасности. Шаблон определяет значения тайм-аутов в соответствии со скоростными параметрами используемой сети. Значения тайм-аутов могут быть откорректированы позднее при настройке сервера безопасности в программе конфигурирования.
- Нажмите кнопку "Далее >".

На экране появится диалог "Название организации".

11. Укажите названия организации и подразделения, которое будет обслуживать устанавливаемый сервер, и нажмите кнопку "Далее >".

Примечание. Эти данные будут использоваться при генерации сертификата сервера безопасности. Названия организации и подразделения могут быть введены позднее или заменены другими при выполнении процедуры "Генерация и установка сертификата сервера безопасности".

На экране появится диалог "Готова к установке программы".

12. Нажмите кнопку "Установить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

После успешной установки и настройки компонентов на экране появится диалог "Программа установки завершена".

13. Нажмите кнопку "Готово" и перезагрузите компьютер.

Установка клиента в сетевом режиме функционирования

Установка клиента в сетевом режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для установки клиента в сетевом режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите установку с помощью команды "Клиентское ПО".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните соответствующее действие:

   - если установку необходимо выполнить на компьютер с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
   - если установку необходимо выполнить на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий. Перед началом процедуры установки на экране появится диалог для выбора режима работы компонента.

2. Установите отметку в поле "Сетевой режим" и нажмите кнопку "Далее >".

   По окончании подготовительных действий на экран будет выведен диалог приветствия программы установки.

3. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".

5. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   На экране появится диалог "Настройка подключения к серверу безопасности".

6. Выберите вариант продолжения процедуры (при наличии в домене хотя бы одного сервера безопасности):

   - с подключением к серверу безопасности — отметьте пункт "связать этот компьютер с сервером и настроить параметры подключения" и заполните поля данными, необходимыми для установления связи данного компьютера с сервером безопасности:
     - в поле "Имя сервера" из раскрывающегося списка выберите имя компьютера, на котором установлен нужный сервер безопасности;
     - в поле "Скорость подключения" из раскрывающегося списка выберите название шаблона сетевых настроек, который соответствует скоростным параметрам используемой сети;

     Примечание. При установке клиента с подключением к серверу безопасности программа установки дополнительно может выдать запрос на использование лицензии продукта. Если на сервере безопасности зарегистрирован подходящий СНК с доступными для использования лицензиями, можно выбрать вариант использования зарегистрированной лицензии либо ввести другой СНК вручную.

   - без подключения к серверу безопасности — отметьте пункт "не связывать этот компьютер с сервером" (в случае такой установки подключить компьютер к серверу безопасности можно позже с помощью программы конфигурирования).

   Примечание. Поля диалога заблокированы для редактирования, если в домене отсутствует компьютер с установленным ПО сервера безопасности.

7. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер".

8. Введите серийный номер клиента.

   Пояснения.

   - Без ввода СНК установка клиента невозможна.
   - Если на шаге 6 выбран сервер безопасности, поле ввода будет автоматически заполнено серийным номером, для которого есть свободные лицензии на данном сервере.

9. При установке клиента на компьютер, который будет использоваться администратором для централизованной настройки параметров механизмов КЦ и ЗПС, а также параметров доменных пользователей, оставьте отмеченным поле "установить средства централизованной настройки". Если на компьютере будут работать только рядовые пользователи — удалите отметку из поля.

Внимание! При выборе варианта без установки средств централизованной настройки, на компьютере будет невозможно использование программы "Контроль программ и данных" в централизованном режиме, а также будут недоступны некоторые функции управления в параметрах доменных пользователей.

10. Для продолжения установки нажмите кнопку "Далее >".

    На экране появится диалог "Папка назначения".

11. Оставьте заданную по умолчанию папку установки клиента или укажите другую папку назначения и нажмите кнопку "Далее >".

    На экране появится диалог "Учетная информация компьютера".

12. Заполните поля диалога учетными данными и нажмите кнопку "Далее >".

    При установке на ОС Windows 2000/XP на экране появится диалог "Дополнительные параметры". Если выполняется установка на другой ОС, на экране появится диалог "Готова к установке программы" — в этом случае пропустите действия **13–14**.

13. При установке на ОС Windows 2000/XP определите необходимость замены установленных по умолчанию прав доступа пользователей к основным ресурсам компьютера. Если требуется заменить права доступа пользователей, оставьте отмеченным поле "выполнить расстановку прав доступа на файлы, каталоги и ключи реестра".

    Пояснения.

    - Замена прав доступа усиливает защищенность операционной системы, однако выполнять ее рекомендуется только в тех случаях, когда после установки ОС администратор не осуществлял специальную расстановку прав доступа. Перечень устанавливаемых прав доступа для соответствующих ОС см. в Приложении на стр. 35 и 37.
    - Права доступа на каталог установки системы Secret Net 6 устанавливаются для любой ОС в обязательном порядке независимо от выбранного режима расстановки прав. Перечень устанавливаемых прав доступа к каталогу установки см. в Приложении на стр. 39.

14. Для продолжения установки нажмите кнопку "Далее >".

    На экране появится диалог "Готова к установке программы".

15. Нажмите кнопку "Установить".

    Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

    В процессе установки ПО на экране могут появляться различные запросы системы. В частности, запросы на выбор нужных действий выводятся в следующих случаях:

    - При установке на ОС Windows Vista и выше перед добавлением в систему драйвера средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card появляется запрос на установку драйвера. Если на данном компьютере такое изделие использоваться не будет, можно отказаться от установки драйвера. При подтверждении установки драйвер регистрируется в системе в качестве самостоятельного компонента (при установке на ОС Windows 2000/XP/2003 драйвер регистрируется по умолчанию). Сведения о средствах аппаратной поддержки см. в документе [8].

- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net 6 может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net 6.

Перед завершением установки требуется выполнить окончательную настройку ПО. Действия для окончательной настройки выполняются в диалоговом окне "Управление Secret Net 6", процедуры работы с которым описаны в документах [3] и [8]. На этапе установки достаточно закрыть диалоговое окно, не внося никаких изменений.

16. После окончательной настройки перезагрузите компьютер.

Внимание! Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Установка средств управления

Установка средств управления выполняется пользователем, входящим в группу администраторов домена.

Перед установкой средств управления необходимо установить на компьютере ПО клиента в сетевом режиме функционирования.

Для установки средств управления:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите установку с помощью команды "Средства управления".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного компакт-диска файл \Setup\OM\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог принятия лицензионного соглашения.

3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее >".

   На экране появится диалог "Папка назначения".

4. Оставьте заданную по умолчанию папку установки средств управления или укажите другую папку и нажмите кнопку "Далее >".

   На экране появится диалог "Готова к установке программы".

5. Нажмите кнопку "Установить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

   После успешной установки и настройки компонентов на экране появится диалог "Программа установки завершена".

6. Нажмите кнопку "Готово" и перезагрузите компьютер.

Глава 2
Обновление и переустановка

Обновление

В системе Secret Net 6 реализована возможность обновления программного обеспечения компонентов с версии 5.0.180.4 и выше на текущую версию. При обновлении сохраняются заданные параметры настройки системы (для некоторых параметров могут быть выставлены значения по умолчанию, если сохранение прежних значений технически невозможно).

Для функционирования компонентов текущей версии системы Secret Net 6 требуются соответствующие серийные номера лицензий. Поэтому для обновления необходимо приобрести нужное количество лицензий на использование компонентов текущей версии. Компоненты предыдущих версий могут продолжать функционировать в системе с ранее приобретенными лицензиями.

Обновление компонентов на компьютерах системы осуществляется по отдельности с помощью программ установки компонентов. Также имеется возможность автоматического обновления клиента на компьютерах системы.

Обновление клиента в автономном режиме функционирования

Обновление клиента в автономном режиме функционирования выполняет администратор безопасности, который должен входить в локальную группу администраторов компьютера.

Предупреждение. Если на компьютере имеются файлы, зашифрованные средствами системы Secret Net предыдущей версии, перед обновлением системы обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен.

Для обновления клиента в автономном режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите обновление с помощью команды "Клиентское ПО".

   Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните соответствующее действие:

   - если установку необходимо выполнить на компьютер с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
   - если установку необходимо выполнить на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

   Примечание. Перед выполнением дальнейших действий рекомендуется завершить работу программы автозапуска, нажав кнопку "Выход" в окне программы.

2. Нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер".

3. Введите серийный номер клиента для автономного режима функционирования и нажмите кнопку "Далее >".

   Пояснение. Без ввода СНК установка клиента невозможна.

   Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению".

4. Нажмите кнопку "Обновить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

В процессе установки ПО на экране могут появляться различные запросы системы. В частности, запросы на выбор нужных действий выводятся в следующих случаях:

- Если не завершена работа программы автозапуска (см. действие 1), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".
- При обновлении на ОС Windows Vista и выше перед добавлением в систему драйвера средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card появляется запрос на установку драйвера. Если на данном компьютере такое изделие использоваться не будет, можно отказаться от установки драйвера. При подтверждении установки драйвер регистрируется в системе в качестве самостоятельного компонента (при обновлении на ОС Windows 2000/XP/2003 драйвер регистрируется по умолчанию). Сведения о средствах аппаратной поддержки см. в документе [8].
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net 6 может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net 6.

По окончании обновления появится диалог "Программа установки завершена".

5. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание! Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Порядок обновления для сетевого режима функционирования

Обновление компонентов в сетевом режиме функционирования системы осуществляется в следующей последовательности:

1. Включите все контроллеры домена.
2. Выполните модификацию AD (см. стр. 12) и дождитесь репликации схемы AD на все контроллеры домена.
3. Обновите ПО сервера безопасности (см. ниже). Если в системе развернута иерархия серверов безопасности, обновление ПО необходимо выполнить последовательно по иерархии, начиная с корневого сервера.
4. Обновите ПО клиента (см. стр. 21) на серверах безопасности и рабочих местах администраторов.
5. Обновите ПО средств управления (см. стр. 22).
6. Обновите ПО клиента (см. стр. 21) в порядке:
   - контроллеры домена;
   - компьютеры сотрудников.

Совет. При большом количестве компьютеров целесообразно применить автоматическое обновление ПО клиента. Сведения о настройке автоматического обновления см. в Приложении на стр. 40.

Обновление сервера безопасности

Обновление сервера безопасности выполняется пользователем, входящим в группу администраторов домена.

Для обновления сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите обновление с помощью команды "Сервер безопасности".

   Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного компакт-диска файл \Setup\Server\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".

3. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   На экране появится диалог "Серийные номера".

4. Введите серийные номера сервера безопасности (СНС), клиента (СНК) и средств управления (СНУ).

   Пояснения.

   - Без ввода СНС установка сервера безопасности невозможна.
   - СНК и СНУ на установку сервера безопасности не влияют. При установке сервера безопасности можно зарегистрировать один или несколько СНК, что позволит в дальнейшем автоматически регистрировать эти номера на клиентах, подчиняемых данному СБ. СНУ вводится, если к данному серверу безопасности планируется подключение программ управления с нескольких рабочих мест одновременно.

5. Нажмите кнопку "Далее >".

   На экране появится диалог "Обновление БД" с запросом параметров учетной записи администратора для подключения к базе данных обновляемого СБ.

6. В поля "Имя пользователя" и "Пароль" введите учетные данные администратора БД и нажмите кнопку "Далее >".

   На экране появится диалог "Программа готова к обновлению".

7. Нажмите кнопку "Обновить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

   По окончании обновления на экране появится диалог "Программа установки завершена".

8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Обновление клиента в сетевом режиме функционирования

Обновление клиента в сетевом режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Предупреждение. Если на компьютере имеются файлы, зашифрованные средствами системы Secret Net предыдущей версии, перед обновлением системы обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен.

Для обновления клиента в сетевом режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите обновление с помощью команды "Клиентское ПО".

   Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните соответствующее действие:

   - если установку необходимо выполнить на компьютер с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
   - если установку необходимо выполнить на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

   Примечание. Перед выполнением дальнейших действий рекомендуется завершить работу программы автозапуска, нажав кнопку "Выход" в окне программы.

2. Нажмите кнопку "Далее >".
3. Если на сервере безопасности, которому подчинен данный клиент, не зарегистрирован СНК текущей версии, на экране появится диалог "Серийный номер" (диалог не появляется при наличии такого СНК на сервере). Введите серийный номер клиента для сетевого режима функционирования и нажмите кнопку "Далее >".

   Пояснение. Без ввода СНК текущей версии установка клиента невозможна.

   На экране появится диалог "Модификация Active Directory".
4. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению".
5. Нажмите кнопку "Обновить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

   В процессе установки ПО на экране могут появляться различные запросы системы. В частности, запросы на выбор нужных действий выводятся в следующих случаях:

   - Если не завершена работа программы автозапуска (см. действие 1), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".

- При обновлении на ОС Windows Vista и выше перед добавлением в систему драйвера средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card появляется запрос на установку драйвера. Если на данном компьютере такое изделие использоваться не будет, можно отказаться от установки драйвера. При подтверждении установки драйвер регистрируется в системе в качестве самостоятельного компонента (при обновлении на ОС Windows 2000/XP/2003 драйвер регистрируется по умолчанию). Сведения о средствах аппаратной поддержки см. в документе [8].
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net 6 может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net 6.

По окончании обновления появится диалог "Программа установки завершена".

6. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание! Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Обновление средств управления

Обновление средств управления выполняется пользователем, входящим в группу администраторов домена.

Для обновления средств управления:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите обновление с помощью команды "Средства управления".

Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного компакт-диска файл \Setup\OM\Setup.exe.

Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Нажмите кнопку "Далее >".

Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению".

3. Нажмите кнопку "Обновить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

По окончании обновления появится диалог "Программа установки завершена".

4. Нажмите кнопку "Готово".

Переустановка (восстановление)

При необходимости можно осуществлять переустановку ПО компонентов системы Secret Net 6. Переустановка применяется для восстановления нарушенной работоспособности системы. Для переустановки следует использовать дистрибутив установленной на компьютере версии компонента.

Переустановка клиента

Переустановка клиента выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для переустановки клиента:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите переустановку с помощью команды "Клиентское ПО".

   Примечание. Запуск процедуры переустановки компонента можно также выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") или путем запуска соответствующего файла:

   - если переустановку необходимо выполнить на компьютере с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
   - если переустановку необходимо выполнить на компьютере с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".

3. Выберите вариант "Исправить" и нажмите кнопку "Далее >".

   При переустановке клиента в сетевом режиме функционирования на экране появится диалог "Модификация Active Directory". Если выполняется переустановка клиента в автономном режиме — перейдите к выполнению действия **5**.

4. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   На экране появится диалог "Готова к исправлению программы".

5. Нажмите кнопку "Установить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

   После успешной установки и настройки компонентов на экране появится диалог "Программа установки завершена".

6. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание! Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Переустановка сервера безопасности

Переустановка сервера безопасности позволяет:

- заменить поврежденные файлы компонента;
- создать новый каталог для размещения резервных копий журналов;
- создать новый каталог для хранения временных файлов;
- восстановить регистрацию компонентов сервера безопасности в AD:
  - возвратить в значения по умолчанию все настройки сервера;

    Примечание. При восстановлении регистрации сервера безопасности в AD с него удаляются все серийные номера.

  - переподчинить один сервер безопасности другому;
  - вывести из подчинения (сделать главным) сервер безопасности;
  - изменить шаблон сетевых настроек сервера безопасности;
  - изменить учетные данные организации и подразделения;
  - заменить в AD и IIS сертификат сервера безопасности.

Переустановка сервера безопасности выполняется пользователем, входящим в группу администраторов домена.

Для переустановки сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net 6. Дождитесь появления окна программы автозапуска (см. стр. 10) и запустите переустановку с помощью команды "Сервер безопасности".

   Примечание. Запуск процедуры переустановки компонента можно также выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") или вручную запустить файл \Setup\Server\Setup.exe с установочного компакт-диска.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
2. Нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".
3. Выберите вариант "Исправить" и нажмите кнопку "Далее >".

   На экране появится диалог "Настройки СУБД".
4. Оставьте прежним или создайте новый каталог для размещения резервных копий журналов и нажмите кнопку "Далее >".

   Примечание. Поле "Имя БД" является информационным и отображает имя базы данных сервера безопасности.

   На экране появится диалог "Настройки ISAPI-расширения".
5. Оставьте прежним или создайте новый каталог для хранения временных файлов и нажмите кнопку "Далее >".

   На экране появится диалог "Регистрация в Active Directory".
6. Выполните следующие действия:
   - Для сохранения в AD имеющейся информации (рекомендуется) — не устанавливайте отметку в поле "восстановить регистрацию компонентов программы в Active Directory" и нажмите кнопку "Далее >.

     На экране появится диалог "Готова к исправлению программы".

     Перейдите к выполнению действия **7**.
   - Для восстановления начальной регистрационной информации сервера в AD — выполните действия, описанные в приложении на стр. 49.

     

     Предупреждение. Режим восстановления регистрации сервера безопасности в AD следует использовать только в крайнем случае, когда другими способами восстановить сервер не удалось.
7. Нажмите кнопку "Установить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

После успешной установки и настройки компонентов на экране появится диалог "Программа установки завершена".

8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Переустановка средств управления

Переустановка средств управления выполняется стандартно и без особенностей. Запуск процедуры переустановки компонента можно выполнить с установочного компакт-диска (см. стр. 17) или стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Глава 3
Удаление

Предупреждение. Если на защищаемых компьютерах имеется конфиденциальная информация, следует принять меры по ее защите после удаления системы Secret Net 6.

Удаление клиента в автономном режиме функционирования

Удаление клиента в автономном режиме функционирования выполняет администратор безопасности, который должен входить в локальную группу администраторов компьютера.

Для удаления клиента в автономном режиме функционирования:

1. В окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") выберите в списке компонент "Secret Net 6" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".
3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".
4. Нажмите кнопку "Удалить".

   Начнется процесс удаления программного обеспечения, завершающийся появлением диалога "Программа установки завершена".
5. Нажмите кнопку "Готово" и перезагрузите компьютер.

Удаление драйвера средства аппаратной поддержки

Если на компьютере установлен драйвер средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card (регистрируется в качестве самостоятельного компонента при установке клиента), удаление драйвера осуществляется отдельно. Запуск процедуры удаления драйвера выполняется стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Порядок удаления для сетевого режима функционирования

Компоненты системы Secret Net 6 в сетевом режиме функционирования, установленные на компьютерах, удаляются по отдельности. Процедуры удаления предусмотрены для следующих компонентов:

- "Secret Net 6";
- "Secret Net 6 — Сервер безопасности";
- "Secret Net 6 — Средства управления".

Для компонента "Модификатор схемы Active Directory" процедура удаления не предусмотрена. Удаление ПО Oracle осуществляется средствами СУБД Oracle.

При удалении компонентов системы Secret Net 6 рекомендуется придерживаться следующей последовательности действий:

1. Удалите ПО средств управления на рабочих местах администраторов.
2. Удалите ПО клиентов на всех компьютерах.
3. Удалите ПО серверов безопасности.
4. Удалите (если требуется) компоненты СУБД Oracle.

Удаление средств управления

Удаление средств управления выполняется стандартно и без особенностей. Запуск процедуры удаления компонента "Secret Net 6 — Средства управления" можно выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Удаление клиента в сетевом режиме функционирования

Удаление клиента в сетевом режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для удаления клиента:

1. В окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") выберите в списке компонент "Secret Net 6" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".

3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".

4. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   Если процедура удаления клиента выполняется на контроллере домена, на экране появится диалог "Дополнительные параметры". При удалении клиента на другом компьютере перейдите к действию **7**.

5. Определите необходимость сохранения параметров системы Secret Net 6 в групповых политиках домена. Для удаления параметров из всех групповых политик установите отметку в поле "удалить групповые политики Secret Net". При необходимости сохранить централизованно заданные параметры удалите отметку из поля.

   Пояснение. Если выбран вариант без удаления, централизованно заданные параметры групповых политик Secret Net 6 продолжают применяться на компьютерах домена с установленным клиентским ПО системы защиты.

6. Нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".

7. Нажмите кнопку "Удалить".

   Начнется процесс удаления программного обеспечения, завершающийся появлением диалога "Программа установки завершена".

8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Удаление драйвера средства аппаратной поддержки

Если на компьютере установлен драйвер средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card (регистрируется в качестве самостоятельного компонента при установке клиента), удаление драйвера осуществляется отдельно. Запуск процедуры удаления драйвера выполняется стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Удаление сервера безопасности

При удалении сервера безопасности следует иметь в виду, что все компьютеры, подчиненные данному серверу, станут "свободными" — то есть не подчиненными какому-либо серверу безопасности.

Удаление сервера безопасности выполняется пользователем, входящим в группу администраторов домена. Пользователь должен иметь права администратора БД.

Для удаления сервера безопасности:

1. В окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") выберите в списке компонент "Secret Net 6 — Сервер безопасности" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".

3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".

4. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   Если у сервера остались подчиненные клиенты, на экране появится запрос на продолжение процедуры удаления.

   

   Рекомендуется прервать процедуру удаления сервера и удалить или переподчинить клиентов, подчиненных данному серверу безопасности.

   Если удаляемый сервер не имеет подчиненных компьютеров или выбран вариант продолжения процедуры удаления, на экране появится диалог "Удаление базы данных".

5. Выполните следующие действия:
   - для сохранения БД — выберите "не удалять базу данных";
   - для удаления БД — выберите "удалить базу данных" и заполните поля "Имя пользователя" и "Пароль" учетными данными пользователя, имеющего право доступа к БД.
   - Нажмите кнопку "Далее >".

   На экране появится диалог "Дополнительно".

6. При необходимости сохранить сертификат сервера безопасности в IIS удалите отметку из поля "удалить сертификат из Internet Information Server" и нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".

7. Нажмите кнопку "Удалить".

   Начнется процесс удаления сервера безопасности, завершающийся появлением диалога "Программа установки завершена".

8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Приложение

Изменения в схеме AD при модификации

Модификатор AD **осуществляет**:

1 **Добавление атрибутов к стандартным классам** "User" **и** "Computer"

Атрибуты, добавляемые к стандартным классам "User" и "Computer", представлены в таблицах Табл. 1 и Табл. 2 ниже.

Табл. 1. Добавляемые атрибуты класса "User"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-User-AccessLevel Назначение: хранение полномочного уровня допуска к конфиденциальной информации OID: 1.2.840.113556.1.8000.1620.1.1.1
2	Наименование атрибута: Infosec-SN-User-fPrintSecretPriv Назначение: хранение привилегии на печать конфиденциальной информации OID: 1.2.840.113556.1.8000.1620.1.1.2
3	Наименование атрибута: Infosec-SN-User-fOutputSecret Назначение: хранение привилегии на вывод конфиденциальной информации OID: 1.2.840.113556.1.8000.1620.1.1.3
4	Наименование атрибута: Infosec-SN-User-fControlLabels Назначение: хранение привилегии на управление категориями конфиденциальности OID: 1.2.840.113556.1.8000.1620.1.1.4
5	Наименование атрибута: Infosec-SN-User-EffectivePublicKey Назначение: хранение текущего открытого криптографического ключа OID: 1.2.840.113556.1.8000.1620.1.1.14
6	Наименование атрибута: Infosec-SN-User-PreviousPublicKey Назначение: хранение предыдущего открытого криптографического ключа OID: 1.2.840.113556.1.8000.1620.1.1.15
7	Наименование атрибута: Infosec-SN-User-EffectiveKeyTimeGenerated Назначение: хранение времени генерации текущего криптографического ключа OID: 1.2.840.113556.1.8000.1620.1.1.16
8	Наименование атрибута: Infosec-SN-User-PreviousKeyTimeGenerated Назначение: хранение времени генерации предыдущего криптографического ключа OID: 1.2.840.113556.1.8000.1620.1.1.17
9	Наименование атрибута: Infosec-SN-User-DBMS-Access-Privilege Назначение: хранение дополнительных флагов OID: 1.2.840.113556.1.8000.1620.1.1.35
10	Наименование атрибута: Infosec-SN-User-ImitSableCompList Назначение: хранение имитовставки списка компьютеров, хранящегося в атрибуте Infosec-SN-User-SableCompList (см. ниже) OID: 1.2.840.113556.1.8000.1620.1.1.41
11	Наименование атрибута: Infosec-SN-User-SableCompList Назначение: хранение списка компьютеров с ПАК "Соболь", доступных данному пользователю OID: 1.2.840.113556.1.8000.1620.1.1.46
12	Наименование атрибута: Infosec-SN-User-AccessCheck Назначение: для проверки маски доступа пользователя к объектам OID: 1.2.840.113556.1.8000.1620.1.1.64
13	Наименование атрибута: Infosec-SS-User-AccessLevel64 Назначение: хранение неиерархической метки доступа (64 бита) OID: 1.2.840.113556.1.8000.1620.1.1.65
14	Наименование атрибута: Infosec-SS-User-Privileges Назначение: хранение привилегий пользователя (все в одном) OID: 1.2.840.113556.1.8000.1620.1.1.66

Табл. 2. Добавляемые атрибуты класса "Computer"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-Computer-OMS-SID Назначение: хранение SID того СБ, которому подчинен данный компьютер OID: 1.2.840.113556.1.8000.1620.1.1.6
2	Наименование атрибута: Infosec-SN-Computer-fAgent Назначение: хранение флага, отображающего наличие Агента на компьютере OID: 1.2.840.113556.1.8000.1620.1.1.19
3	Наименование атрибута: Infosec-SN-Computer-Shedule Назначение: хранение расписания сбора журналов для данного компьютера OID: 1.2.840.113556.1.8000.1620.1.1.22
4	Наименование атрибута: Infosec-SN-Computer-fLogLogon Назначение: хранение флага сбора журналов для данного компьютера при его подключении к СБ OID: 1.2.840.113556.1.8000.1620.1.1.26
5	Наименование атрибута: Infosec-SN-Computer-HttpTransportSettings Назначение: хранение настроек транспортной подсистемы для данного компьютера OID: 1.2.840.113556.1.8000.1620.1.1.34
6	Наименование атрибута: Infosec-SN-Computer-SablePublicKey Назначение: хранение открытого ключа компьютера OID: 1.2.840.113556.1.8000.1620.1.1.42
7	Наименование атрибута: Infosec-SN-Computer-SableVK Назначение: хранение дополнительных данных для расчета ключа SComp OID: 1.2.840.113556.1.8000.1620.1.1.43
8	Наименование атрибута: Infosec-SN-Computer-SableKeyInfoImit Назначение: хранение имитовставки от блоба CompKeyInfo (PKk + VK) OID: 1.2.840.113556.1.8000.1620.1.1.44
9	Наименование атрибута: Infosec-SN-Computer-SableSyncData Назначение: хранение данных синхронизации Соболя OID: 1.2.840.113556.1.8000.1620.1.1.45
10	Наименование атрибута: Infosec-SN-Computer-AgentFlags Назначение: хранение управляющих флагов Агента OID: 1.2.840.113556.1.8000.1620.1.1.50
11	Наименование атрибута: Infosec-SN-Computer-SablePlantNumber Назначение: хранение заводского номера платы ПАК "Соболь" OID: 1.2.840.113556.1.8000.1620.1.1.59
12	Наименование атрибута: Infosec-SN-Computer-RegWSDepartement Назначение: хранение учетной информации компьютера (название подразделения) OID: 1.2.840.113556.1.8000.1620.1.1.60
13	Наименование атрибута: Infosec-SN-Computer- RegWSSystem Назначение: хранение учетной информации компьютера (название автоматизированной системы) OID: 1.2.840.113556.1.8000.1620.1.1.61
14	Наименование атрибута: Infosec-SN-Computer- RegWSLocation Назначение: хранение учетной информации компьютера (расположение компьютера) OID: 1.2.840.113556.1.8000.1620.1.1.62
15	Наименование атрибута: Infosec-SN-Computer- RegWSNumber Назначение: хранение учетной информации компьютера (номер системного блока) OID: 1.2.840.113556.1.8000.1620.1.1.63
16	Наименование атрибута: Infosec-SS-Computer-SnProductInfo Назначение: для хранения информации об установленном продукте OID: 1.2.840.113556.1.8000.1620.1.1.67
17	Наименование атрибута: Infosec-SN-Computer-ClientSN-Item Назначение: для хранения серийного номера текущего клиента OID: 1.2.840.113556.1.8000.1620.1.1.69
18	Наименование атрибута: Infosec-SN-Computer-ServiceSN Назначение: для хранения списка серийных номеров служб (лицензирование SS 1.0) OID: 1.2.840.113556.1.8000.1620.1.1.70
19	Наименование атрибута: Infosec-SN-Computer-ClientSN61 Назначение: для хранения серийного номера текущего клиента (лицензирование SN 6.1) OID: 1.2.840.113556.1.8000.1620.1.1.74

2 Добавление новых классов с соответствующими атрибутами

- **класс "Infosec-SN-ADSchema"**
  класс предназначен для хранения информации о текущей схеме AD и имеет OID 1.2.840.113556.1.8000.1620.1.2.1 (атрибуты см. в Табл. 3).

Табл. 3. Добавляемые атрибуты класса "Infosec-SN-Schema"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-ADSchema-Version Назначение: хранение основного номера текущей версии схемы AD OID: 1.2.840.113556.1.8000.1620.1.1.5
2	Наименование атрибута: Infosec-SN-ADSchema-VersionExtended Назначение: хранение расширенного номера текущей версии схемы AD OID: 1.2.840.113556.1.8000.1620.1.1.54

- **класс "Infosec-SN-OMS"**
  класс предназначен для хранения информации о серверах безопасности и имеет OID: 1.2.840.113556.1.8000.1620.1.2.2 (атрибуты см. в Табл. 4 ниже).

Табл. 4. Добавляемые атрибуты класса "Infosec-SN-OMS"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-OMS-SID Назначение: хранение SID данного СБ OID: 1.2.840.113556.1.8000.1620.1.1.7
2	Наименование атрибута: Infosec-SN-OMS-ParentSID Назначение: хранение SID родительского СБ в иерархии СБ (родительского для СБ, SID которого хранится в предыдущем атрибуте) OID: 1.2.840.113556.1.8000.1620.1.1.8
3	Наименование атрибута: Infosec-SN-OMS-Certificate Назначение: хранение X.509 сертификата СБ OID: 1.2.840.113556.1.8000.1620.1.1.9
4	Наименование атрибута: Infosec-SN-OMS-Shedule Назначение: хранение расписания сбора журналов для подчиненных данному СБ рабочих станций OID: 1.2.840.113556.1.8000.1620.1.1.25
5	Наименование атрибута: Infosec-SN-OMS-fLogLogon Назначение: хранение флага сбора журналов для подчиненных данному СБ рабочих станций при их подключении к СБ OID: 1.2.840.113556.1.8000.1620.1.1.27
6	Наименование атрибута: Infosec-SN-OMS-SecurityDescriptor Назначение: хранение дескриптора безопасности для СБ OID: 1.2.840.113556.1.8000.1620.1.1.32
7	Наименование атрибута: Infosec-SN-OMS-HttpTransportSettings Назначение: хранение настроек транспорта для СБ OID: 1.2.840.113556.1.8000.1620.1.1.33
8	Наименование атрибута: Infosec-SN-OMS-MailSettings Назначение: хранение правил почтовой рассылки уведомлений о событиях НСД для данного СБ OID: 1.2.840.113556.1.8000.1620.1.1.36
9	Наименование атрибута: Infosec-SN-OMS-ClientSN Назначение: хранение серийных номеров клиентов (лицензирование SN 5.0) OID: 1.2.840.113556.1.8000.1620.1.1.37
10	Наименование атрибута: Infosec-SN-OMS-ManagementSN Назначение: хранение серийных номеров программ управления (лицензирование SN 5.0) OID: 1.2.840.113556.1.8000.1620.1.1.38
11	Наименование атрибута: Infosec-SN-OMS-ADQueryTimeOut Назначение: хранение тайм-аута, задающего периодичность опроса AD данным СБ для считывания настроек OID: 1.2.840.113556.1.8000.1620.1.1.51
12	Наименование атрибута: Infosec-SN-OMS-ArchiveJournalSchedule Назначение: хранение расписания архивирования журналов OID: 1.2.840.113556.1.8000.1620.1.1.52

№ п/п	Атрибут
13	Наименование атрибута: Infosec-SN-OMS-Config Назначение: хранение настроек для данного СБ OID: 1.2.840.113556.1.8000.1620.1.1.53
14	Наименование атрибута: Infosec-SN-OMS-Flags Назначение: хранение управляющих флагов СБ OID: 1.2.840.113556.1.8000.1620.1.1.55
15	Наименование атрибута: Infosec-SN-OMS-ClientSNEx Назначение: хранение серийных ключей клиентов (лицензирование SN 5.1) OID: 1.2.840.113556.1.8000.1620.1.1.71
16	Наименование атрибута: Infosec-SN-OMS- ManagementSNEx Назначение: хранение серийных ключей программ управления (лицензирование SN 5.1) OID: 1.2.840.113556.1.8000.1620.1.1.72
17	Наименование атрибута: Infosec-SN-OMS-ServerSN Назначение: хранение серийного номера сервера безопасности (лицензирование SN 5.1) OID: 1.2.840.113556.1.8000.1620.1.1.73
18	Наименование атрибута: Infosec-SN-OMS-ClientSN61 Назначение: хранение серийных ключей клиентов (лицензирование SN 6.1) OID: 1.2.840.113556.1.8000.1620.1.1.75
19	Наименование атрибута: Infosec-SN-OMS-ManagementSN61 Назначение: хранение серийных ключей программ управления (лицензирование SN 6.1) OID: 1.2.840.113556.1.8000.1620.1.1.76
20	Наименование атрибута: Infosec-SN-OMS-ServerSN61 Назначение: хранение серийного номера сервера безопасности (лицензирование SN 6.1) OID: 1.2.840.113556.1.8000.1620.1.1.77

- **класс "Infosec-SN-UEI"**
  класс предназначен для хранения информации об ЭИ пользователя и имеет OID: 1.2.840.113556.1.8000.1620.1.2.3 (атрибуты см. в Табл. 5).

Табл. 5. Добавляемые атрибуты класса "Infosec-SN-UEI"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-UEI-UserSID Назначение: хранение SID пользователя OID: 1.2.840.113556.1.8000.1620.1.1.10
2	Наименование атрибута: Infosec-SN-UEI-Type Назначение: хранение типа электронного идентификатора (ЭИ) OID: 1.2.840.113556.1.8000.1620.1.1.11
3	Наименование атрибута: Infosec-SN-UEI-Size Назначение: хранение размера ID ЭИ, хранимого в следующем атрибуте OID: 1.2.840.113556.1.8000.1620.1.1.12
4	Наименование атрибута: Infosec-SN-UEI-Id Назначение: хранение ID электронного идентификатора OID: 1.2.840.113556.1.8000.1620.1.1.13
5	Наименование атрибута: Infosec-SN-UEI-Flags Назначение: хранение флагов электронного идентификатора OID: 1.2.840.113556.1.8000.1620.1.1.18
6	Наименование атрибута: Infosec-SN-UEI-AuthInfo Назначение: хранение информации об аутентификаторе OID: 1.2.840.113556.1.8000.1620.1.1.39

- **класс "Infosec-SN-GSableData"**
  класс предназначен для хранения глобальной информации о проверке ключей ЦУ ПАК "Соболь" и имеет OID 1.2.840.113556.1.8000.1620.1.2.4 (атрибуты см. в Табл. 6).

Табл. 6. Добавляемые атрибуты класса "Infosec-SN-GSableData"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-GSableData-KeysCheckData Назначение: хранение случайной последовательности для проверки ключей ЦУ ПАК "Соболь" OID: 1.2.840.113556.1.8000.1620.1.1.47
2	Наименование атрибута: Infosec-SN-GSableData-KaCheckImit Назначение: хранение имитовставки случайной последовательности на ключе Ka OID: 1.2.840.113556.1.8000.1620.1.1.48
3	Наименование атрибута: Infosec-SN-GSableData-SKaCheckImit Назначение: хранение имитовставки случайной последовательности на ключе SKa OID: 1.2.840.113556.1.8000.1620.1.1.49

- **классы "Infosec-SN-ICheckObj" и "Infosec-SN-ICheckObj64"**
  классы предназначены для хранения информации об объектах ЦУ КЦ ЗПС и имеют OID 1.2.840.113556.1.8000.1620.1.2.5 и 1.2.840.113556.1.8000.1620.1.2.7 (атрибуты см. в Табл. 7).

Табл. 7. Добавляемые атрибуты классов "Infosec-SN-ICheckObj" и "Infosec-SN-ICheckObj64"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-ICheckObj-ID Назначение: хранение идентификатора объекта ЦУ КЦ ЗПС OID: 1.2.840.113556.1.8000.1620.1.1.56
2	Наименование атрибута: Infosec-SN-ICheckObj-Type Назначение: хранение типа объекта ЦУ КЦ ЗПС OID: 1.2.840.113556.1.8000.1620.1.1.57
3	Наименование атрибута: Infosec-SN-ICheckObj-Data Назначение: хранение данных объекта ЦУ КЦ ЗПС OID: 1.2.840.113556.1.8000.1620.1.1.58

- **класс "Infosec-SS-GClientInfo"**
  класс предназначен для хранения глобальной информации об установленных в системе продуктах линеек Secret Net 6 и Secret Net 5 и имеет OID 1.2.840.113556.1.8000.1620.1.2.6 (атрибуты см. в Табл. 8).

Табл. 8. Добавляемые атрибуты класса "Infosec-SS-GClientInfo"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SS-GClientInfo-ProductTypes Назначение: хранение информации об установленных типах продуктов OID: 1.2.840.113556.1.8000.1620.1.1.68

3 Создание конфигурационной информации

Конфигурационная информация для установленного продукта создается в разделе Конфигурации каталога AD.

В этом разделе создаются следующие объекты:

- В контейнере "Services" создается служебный контейнер "SecretNet 5.0 Configuration".
- В контейнере "SecretNet 5.0 Configuration" создается объект ADSchema (класс Infosec-SN-ADSchema), хранящий текущую версию схемы AD.

  После проведения модификации текущая версия схемы AD хранится в разделе конфигурации, что позволяет после проведения очередной репликации иметь доступ к этой информации в рамках всего леса.

- В контейнерах "CN=409, CN=DisplaySpecifiers" и "CN=419, CN=DisplaySpecifiers" создаются конфигурационные данные для поддержки управляющих модулей системы:
  - в атрибут adminContextMenu объектов user-Display и inetOrgPerson-Display добавляется GUID {26DFFB2F-9AA6-4219-8287-88489C3E55F0} для обработки операций смены пароля пользователя в контекстном меню;
  - в атрибут adminPropertyPages объектов user-Display и inetOrgPerson-Display добавляется GUID {2F01C0A1-E5DD-496c-AA30-196A26D3B1C2} для отображения дополнительной страницы свойств при управлении параметрами пользователей;
  - в атрибут dSUIAdminNotification объекта DS-UI-Default-Settings добавляется GUID {26DFFB2F-9AA6-4219-8287-88489C3E55F0} для получения уведомления при удалении пользователя;
  - в атрибут dSUIAdminNotification объекта DS-UI-Default-Settings добавляется GUID {CDB5CE54-B162-48bd-968F-A9CA4E81F31E}, обеспечивающий пункт "Загрузить ключи ЦУ" в контекстном меню объекта "User" (при выборе этого пункта запускается загрузка ключей ЦУ ПАК "Соболь").

Расстановка прав доступа в ОС Windows 2000

Права доступа на каталоги и файлы

Имя объекта	Права доступа
%SystemDrive%\	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
C:\autoexec.bat	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
C:\boot.ini	Administrators: FullControl SYSTEM: FullControl
C:\config.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
C:\ntbootdd.sys	Administrators: FullControl SYSTEM: FullControl
C:\ntdetect.com	Administrators: FullControl SYSTEM: FullControl
C:\ntldr	Administrators: FullControl SYSTEM: FullControl
C:\io.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
C:\msdos.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\autoexec.bat	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\boot.ini	Administrators: FullControl SYSTEM: FullControl
%SystemDrive%\config.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\ntbootdd.sys	Administrators: FullControl SYSTEM: FullControl
%SystemDrive%\ntdetect.com	Administrators: FullControl SYSTEM: FullControl
%SystemDrive%\ntldr	Administrators: FullControl SYSTEM: FullControl
%SystemDrive%\io.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\msdos.sys	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemRoot%	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemRoot%\$NtServicePackUninstall$	Administrators: FullControl SYSTEM: FullControl
%SystemRoot%\debug	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemRoot%\debug\UserMode	Administrators: FullControl SYSTEM: FullControl Users: Create files, Create folders (Files Only) Users: Traverse folder, List folder, Create files (Folder Only)

Имя объекта	Права доступа
%SystemRoot%\Registration	Administrators: FullControl SYSTEM: FullControl Users: Read
%SystemRoot%\repair	Administrators: FullControl SYSTEM: FullControl
%SystemRoot%\Temp	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Traverse folder, Create files, Create folders (Folder & subfoldres)
%SystemRoot%\regedit.exe	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\appmgmt	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\config	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\dllcache	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl
%SystemDirectory%\DTCLog	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\GroupPolicy	Administrators: FullControl Authenticated Users: Read, Execute SYSTEM: FullControl
%SystemDirectory%\ias	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl
%SystemDirectory%\NTMSData	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\repl	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\repl\export	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) Replicator: Read, Execute, Delete SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\repl\import	Administrators: FullControl Replicator: Modify SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\Setup	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDirectory%\spool\Printers	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (Folder & subfolders)
%SystemDirectory%\Ntbackup.exe	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\rcp.exe	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\Regedt32.exe	Administrators: FullControl SYSTEM: FullControl

Имя объекта	Права доступа
%SystemDirectory%\rexec.exe	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\rsh.exe	Administrators: FullControl SYSTEM: FullControl
%SystemDirectory%\secedit.exe	Administrators: FullControl SYSTEM: FullControl
%ProgramFiles%	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\Documents and Settings	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\Documents and Settings\ Administrator	Administrator: FullControl SYSTEM: FullControl
%SystemDrive%\Documents and Settings\ All Users	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Traverse folder, Create files, Create folders (Folder & subfoldres)
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson\drwtsn32.log	Administrators: FullControl SYSTEM: FullControl Users: Modify
%SystemDrive%\Temp	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Traverse folder, Create files, Create folders (Folder & subfoldres)

Примечание. %SystemDirectory% — это %SystemRoot%\system32

Права доступа на ключи реестра

Ключ	Права доступа	Наследование
HKLM\SOFTWARE	Administrators: FullControl CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет
HKLM\SOFTWARE\Classes	Administrators: FullControl Authenticated Users: Read CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет
HKLM\SOFTWARE\Classes\.hlp	Administrators: FullControl Authenticated Users: Read CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет
HKLM\SOFTWARE\Classes\helpfile	Administrators: FullControl Authenticated Users: Read CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет
HKLM\SOFTWARE\ Microsoft\OS/2 Subsystem for NT	Administrators: FullControl CREATOR OWNER: FullControl (Subkeys) SYSTEM: FullControl	Нет

Ключ	Права доступа	Наследование
HKLM\SOFTWARE\ Microsoft\ Windows NT\CurrentVersion	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControl- Set\Control\ComputerName	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Control\ ContentIndex	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Control\ Keyboard Layout	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Control\ Keyboard Layouts	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Control\Print\ Printers	Administrators: FullControl Authenticated Users: Read CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет
HKLM\SYSTEM\ CurrentControlSet\Control\ ProductOptions	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Services\ EventLog	Authenticated Users: Read	Да
HKLM\SYSTEM\ CurrentControlSet\Services\Tcpip	Authenticated Users: Read	Да
HKEY_CLASSES_ROOT	Administrators: FullControl Authenticated Users: Read CREATOR OWNER: FullControl (Subkeys) Power Users: Special (Read, Write, Delete) SYSTEM: FullControl Users: Read	Нет

Расстановка прав доступа в ОС Windows XP

Права доступа на каталоги и файлы

Имя объекта	Права доступа
%SystemDrive%\	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\ Documents and Settings	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Read, Execute
%AllUsersProfile%	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%AllUsersProfile%\ Application Data\Microsoft	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Travers Folder, Execute File List Folder, Read Data, Read Attributes, Read Extended Attributes, Create Files, Write Data, Create Folders, Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Read Permissions
%AllUsersProfile%\Application Data\Microsoft\ Crypto\DSS\MachineKeys	Administrators: FullControl SYSTEM: FullControl Users: List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (Folder Only)
%AllUsersProfile%\Application Data\ Microsoft\HTML Help	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Modify
%AllUsersProfile%\Application Data\ Microsoft\Media Index	Administrators: FullControl SYSTEM: FullControl Users: Create files, Create folders, Write attributes, Write extended attributes, Read permissions (Folder only) Users: Write (Subfolders & files) Users: Read, Execute Power Users: Traverse Folder, Execute File List Folder, Read Data, Read Attributes, Read Extended Attributes, Create Files, Write Data, Create Folders, Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Read Permissions
%SystemDrive%\ Documents and Settings\ Default User	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Read, Execute
%SystemRoot%\Installer	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemRoot%\Registration	Administrators: FullControl (Folder & files) SYSTEM: FullControl (Folder & files) Users: Read (Folder & files)

Права доступа на каталог установки клиента

Имя объекта	Права доступа
%InstallDir% [1)]	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%InstallDir%\icheck	Administrators: FullControl SYSTEM: FullControl

[1)] — по умолчанию %Program Files%\Secret Net\Client.

Изменения в реестре при установке клиента

Программа установки компонента "Secret Net 6" вносит следующие изменения в стандартные параметры реестра:

Имя параметра	Тип	Значение
раздел HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\		
EnableICMPRedirect	DWORD	0
SynAttackProtect	DWORD	2
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery	DWORD	0
KeepAliveTime	DWORD	300,000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5
раздел HKLM\System\CurrentControlSet\Services\AFD\Parameters\		
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000
раздел HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\		
NoDriveTypeAutoRun	DWORD	0xFF

Настройка автоматической установки и обновления ПО клиента

Если система состоит из большого количества компьютеров, установка программного обеспечения занимает значительное время. Для оптимизации процесса развертывания системы предоставляется возможность автоматической установки и обновления компонента "Secret Net 6".

Автоматическая установка и обновление ПО клиента осуществляются на компьютерах определенных организационных подразделений. На каждом компьютере запуск процесса установки или обновления происходит автоматически при загрузке операционной системы до входа пользователя в систему. Если на компьютере не найдено установленное ПО клиента — запускается процесс установки. При обнаружении компонента предыдущей версии — выполняется обновление на текущую версию ПО.

Внимание! При автоматической установке/обновлении клиента не выполняется установка или обновление драйвера средства аппаратной поддержки Secret Net Card. Драйвер, оставшийся от предыдущей версии Secret Net, не удаляется из системы программой установки и не будет работать корректно с новой версией системы. После завершения автоматической установки или обновления выполните установку драйвера вручную на нужных компьютерах. Для установки драйвера запустите файл "Драйвер платы Secret Net Touch Memory Card.msi" из соответствующего каталога на установочном компакт-диске:

- \Setup\SnTmCard\Win32\ — для 32-разрядных версий ОС Windows;
- \Setup\SnTmCard\x64\ — для 64-разрядных версий ОС Windows.

Процедура настройки системы для автоматической установки и обновления состоит из следующих этапов:

1. Создание общедоступного сетевого ресурса.
2. Создание файлов со сценарием установки.
3. Создание организационных подразделений и включение в них компьютеров.
4. Создание групповых политик для организационных подразделений.
5. Включение автоматической установки и обновления.

Создание общедоступного сетевого ресурса

В домене необходимо создать общедоступный сетевой ресурс (ОСР), содержащий файлы для установки ПО клиента.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте общий доступ к этой папке.

   Примечание. Необходимо обеспечить доступность компьютера для сетевых обращений во время проведения автоматической установки ПО. Рекомендуется создать ОСР на одном из файловых серверов домена.

2. С установочного компакт-диска системы Secret Net 6 скопируйте в папку содержимое следующих каталогов (сохраняя их структурную вложенность):

Имя каталога	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Tools\Microsoft\	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах будет выполнена без установки соответствующих обновлений ОС

Создание файлов со сценарием установки

Сценарии предназначены для автоматизации процесса установки клиентского программного обеспечения. Они позволяют частично или полностью автоматизировать ввод информации, запрашиваемой программой установки клиента.

Файлы со сценарием установки создаются в XML-формате (кодировка "windows-1251") и помещаются в общедоступном сетевом ресурсе в каталогах \Setup\Client\Win32 и \Setup\Client\x64. Создать файл сценария можно с использованием программы установки клиента или вручную.

Для создания файла сценария с помощью программы установки:

1. На компьютере без установленного ПО клиента создайте на локальном диске папку для временного размещения дистрибутивных файлов.
2. С установочного компакт-диска системы Secret Net 6 скопируйте в папку содержимое следующих каталогов (сохраняя их структурную вложенность):

Имя каталога	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Tools\Microsoft\	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах будет выполнена без установки соответствующих обновлений ОС

3. Запустите консоль командной строки (cmd.exe).
4. Введите команду для запуска программы установки клиента в режиме создания файла сценария:
   - на компьютере под управлением 32-разрядной версии Windows: start <*имя_папки*>\Setup\Client\Win32\Setup.exe /script:3
   - на компьютере под управлением 64-разрядной версии Windows: start <*имя_папки*>\Setup\Client\x64\Setup.exe /script:3

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
5. Нажмите кнопку "Далее >" и выполните предлагаемые программой действия до появления диалога "Готова к установке программы".

   Пояснение. Программа установки функционирует как в обычном режиме, при этом полученные программой данные протоколируются и на определенном этапе сохраняются в файле сценария. Файл сценария создается программой до начала непосредственной установки ПО на компьютер, поэтому после создания файла работу программы установки можно завершить.
6. В диалоге "Готова к установке программы" нажмите кнопку "Отмена" и подтвердите решение о прекращении установки в появившемся диалоге запроса.

   На экране появится диалог "Программа установки завершена".
7. Нажмите кнопку "Готово" и проверьте наличие в папке файла сценария SnInstall.script. Скопируйте файл в подкаталоги \Setup\Client\Win32 и \Setup\Client\x64 папки ОСР.

Для создания файла сценария вручную:

- В текстовом редакторе создайте файл SnInstall.script, сформируйте содержимое документа по правилам языка XML и сохраните файл в подкаталогах \Setup\Client\Win32 и \Setup\Client\x64 папки ОСР.

Структура файла сценария:

```
<?xml version="1.0" encoding="windows-1251"?>
<SnInstallScript>
    <DB>
        <Property>
            <параметр_1>значение_параметра</параметр_1>
            <параметр_2>значение_параметра</параметр_2>
            ...
            <параметр_N>значение_параметра</параметр_N>
        </Property>
    </DB>
</SnInstallScript>
```

В группе Property указываются параметры и их значения, необходимые программе установки ПО клиента. Перечень основных параметров, предусмотренных для редактирования, представлен в таблице.

Параметр	Значение по умолчанию	Описание
INSTALLDIR	\Program Files\Secret Net\Client	Путь установки ПО клиента
REBOOT	Force	Определяет необходимость перезагрузки компьютера после установки: • "Force" – перезагрузка должна выполняться; • "ReallySuppres" – перезагрузка не выполняется, даже если она нужна для работы ПО.
SNSETPERMISSIONS	0 — для Windows 2003 1 — для Windows 2000/XP	Определяет необходимость замены прав доступа пользователей к основным ресурсам компьютера: • "0" — замена прав не выполняется; • "1" — замена прав будет выполняться.
SNADMANAGERACCOUNTNAME	Отсутствует	Имя учетной записи для доступа к AD
SNADMANAGERPASSWORD	Отсутствует	Пароль учетной записи для доступа в AD
SNSERIALNUMBER	Отсутствует	Серийный номер клиента
SNDIVISION	Отсутствует	Учетная информация компьютера: название подразделения
SNAUTOSYSTEMNAME	Отсутствует	Учетная информация компьютера: название автоматизированной системы
SNPCLOCATION	Отсутствует	Учетная информация компьютера: рабочее место
SNPCSERIAL	Отсутствует	Учетная информация компьютера: номер системного блока

Если параметру не присвоено значение, будет использоваться значение, заданное по умолчанию. Обязательно должны быть указаны значения для следующих параметров: INSTALLDIR и SNSERIALNUMBER.

Для задания пути допускается использование переменных. Имя переменной задается в квадратных скобках и должно находиться в начале значения параметра. Перечень поддерживаемых переменных представлен в таблице.

Переменная	Пример значения
WindowsVolume	C:\
WindowsFolder	C:\WINDOWS\
USERPROFILE	C:\Documents and Settings\Ivanov\
TemplateFolder	C:\Documents and Settings\All Users\Templates\
TempFolder	C:\Documents and Settings\Ivanov\Local Settings\Temp
SystemFolder	C:\WINDOWS\system32\
StartupFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\
StartMenuFolder	C:\Documents and Settings\All Users\Start Menu
SendToFolder	C:\Documents and Settings\Ivanov\SendTo\

Переменная	Пример значения
ProgramMenuFolder	C:\Documents and Settings\All Users\Start Menu\Programs\
PrimaryVolumePath	C:\
PersonalFolder	C:\Documents and Settings\Ivanov\My Documents\
MyPicturesFolder	C:\Documents and Settings\Ivanov\My Documents\My Pictures\
LocalAppDataFolder	C:\Documents and Settings\Ivanov\Local Settings\Application Data\
FontsFolder	C:\WINDOWS\Fonts\
FavoritesFolder	C:\Documents and Settings\Ivanov\Favorites\
CommonFilesFolder	C:\Program Files\Common Files\
CommonAppDataFolder	C:\Documents and Settings\All Users\Application Data\
ProgramFilesFolder	C:\Program Files\
AppDataFolder	C:\Documents and Settings\Ivanov\Application Data
AdminToolsFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\
ALLUSERSPROFILE	C:\Documents and Settings\All Users

Пример содержимого файла сценария:

```
<?xml version="1.0" encoding="windows-1251"?>
<SnInstallScript>
    <DB>
        <Property>
            <INSTALLDIR>
                [ProgramFilesFolder]Secret Net\Client
            </INSTALLDIR>
            <REBOOT>Force</REBOOT>
            <SNSETPERMISSIONS></SNSETPERMISSIONS>
            <SNADMANAGERACCOUNTNAME>
                domainname\V_Ivanov
            </SNADMANAGERACCOUNTNAME>
            <SNADMANAGERPASSWORD>
                12345678
            </SNADMANAGERPASSWORD>
            <SNSERIALNUMBER>
                1234-5678-9123-4567-8901-2345-6789
            </SNSERIALNUMBER>
        </Property>
    </DB>
</SnInstallScript>
```

В приведенном примере предписывается:

- установить продукт в папку программ на системном диске в каталоге \Secret Net\Client;
- перезагрузить компьютер после установки;
- для доступа к AD использовать учетную запись "domainname\V_Ivanov" с паролем "12345678";
- для установки продукта использовать серийный номер:

  "1234-5678-9123-4567-8901-2345-6789".

Создание организационных подразделений

Чтобы выделить компьютеры домена, на которых будет выполняться автоматическая установка или обновление ПО, необходимо создать организационные подразделения (Organization Units) и включить в них нужные компьютеры. Также можно использовать имеющиеся организационные подразделения.

Создание организационных подразделений и добавление объектов осуществляется стандартными способами.

Создание групповых политик

Для подготовленных организационных подразделений необходимо создать групповые политики автоматической установки ПО. Групповые политики создаются отдельно для 32- и 64-разрядных версий ОС Windows.

После того как автоматическая установка ПО будет выполнена на всех компьютерах, созданные групповые политики можно отключить или удалить стандартными способами.

Для создания групповой политики на контроллере домена под управлением ОС Windows 2008 (нерусифицированная версия):

1. Вызовите консоль "Group Policy Management".
2. Вызовите контекстное меню организационного подразделения, на компьютерах которого будет проводиться автоматическая установка, и активируйте команду "Create a GPO in this domain, and Link it here".
3. В появившемся диалоге введите имя создаваемой политики и нажмите кнопку "OK".

   Новая политика появится в иерархическом списке в качестве подчиненного объекта организационного подразделения.
4. Вызовите контекстное меню политики и активируйте команду "Edit".

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Computer Configuration\Policies\Windows Settings\Scripts" и вызовите диалоговое окно настройки свойств параметра "Startup".
6. В диалоговом окне нажмите кнопку "Add".

   На экране появится диалог "Add a Script".
7. В поле "Script Name" введите нужное значение:
   - для применения политики на компьютерах с 32-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\Win32\Setup.exe
   - для применения политики на компьютерах с 64-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\x64\Setup.exe
8. В поле "Script Parameters" введите значение /autoinstall
9. Нажмите кнопку "OK", затем в диалоговом окне последовательно нажмите кнопки "Apply" и "OK" и закройте остальные окна.

Совет. Если используются несколько организационных подразделений для автоматической установки ПО, создавать отдельные групповые политики для каждого подразделения необязательно. В остальных подразделениях можно добавить ссылку на созданные групповые политики (с помощью команды контекстного меню "Link an Existing GPO").

Для создания групповой политики на контроллере домена под управлением ОС Windows 2000/2003 (русифицированная версия):

1. Откройте оснастку "Active Directory — Пользователи и Компьютеры", выберите организационное подразделение, на компьютерах которого будет проводиться автоматическая установка, и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика" и нажмите кнопку "Создать".
3. Введите имя создаваемой политики и нажмите клавишу <Enter>.
4. Нажмите кнопку "Изменить".

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Автозагрузка".
6. В диалоговом окне нажмите кнопку "Добавить".

   На экране появится диалог "Добавление сценария".

7. В поле "Имя сценария" введите нужное значение:
   - для применения политики на компьютерах с 32-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\Win32\Setup.exe
   - для применения политики на компьютерах с 64-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\x64\Setup.exe
8. В поле "Параметры сценария" введите значение /autoinstall
9. Нажмите кнопку "ОК", затем в диалоговом окне настройки свойств последовательно нажмите кнопки "Применить" и "ОК" и закройте остальные окна.

Совет. Если используются несколько организационных подразделений для автоматической установки ПО, создавать отдельные групповые политики для каждого подразделения необязательно. В остальных подразделениях можно добавить ссылку на созданные групповые политики (для этого используйте кнопку "Добавить" на вкладке "Групповая политика" в окне настройки свойств организационного подразделения).

Включение автоматической установки и обновления

Выполнение автоматической установки и обновления ПО на компьютерах начинается после включения действия созданных групповых политик.

Для включения действия групповой политики на контроллере домена под управлением ОС Windows 2008 (нерусифицированная версия):

1. Вызовите консоль "Group Policy Management".
2. Вызовите контекстное меню политики, созданной для организационного подразделения, на компьютерах которого будет проводиться автоматическая установка, и активируйте команду "Edit".

   На экране появится окно редактора групповых политик.
3. В дереве объектов политики перейдите к разделу "Computer Configuration\Policies\Administrative Templates...\System\Group Policy" и вызовите диалоговое окно настройки свойств параметра "Scripts policy processing".
4. Установите отметку в поле "Enabled" и затем отметьте следующие параметры:
   - "Do not apply during periodic background processing".
   - "Process even if the Group Policy objects have not changed".
5. Нажмите кнопку "ОК".
6. Задайте значения параметров, как указано в таблице.

Табл. 9. Параметры для ОС Windows Server 2008

Раздел дерева объектов	Параметр	Значение
Computer Configuration\Policies\Administrative Templates...\System\Logon	Always wait for the network at computer startup and logon	Включен
Computer Configuration\Policies\Administrative Templates...\System\Scripts	Run startup scripts asynchronously	Отключен

Для включения действия групповой политики на контроллере домена под управлением ОС Windows 2000/2003 (русифицированная версия):

1. Откройте оснастку "Active Directory — Пользователи и Компьютеры", выберите организационное подразделение, на компьютерах которого будет проводиться автоматическая установка, и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика", выберите политику автоматической установки ПО и нажмите кнопку "Изменить".

   На экране появится окно редактора групповых политик.
3. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Административные шаблоны\System\Group Policy" и вызовите диалоговое окно настройки свойств параметра "Scripts policy processing".

4. Установите отметку в поле "Включен" и затем отметьте следующие параметры:
   - "Do not apply during periodic background processing".
   - "Process even if the Group Policy objects have not changed".
5. Нажмите кнопку "ОК".
6. В зависимости от типа операционной системы задайте значения параметров, как указано в соответствующей таблице.

Табл. 10. Параметры для ОС Windows Server 2003

Раздел дерева объектов	Параметр	Значение
Конфигурация компьютера\ Административные шаблоны\ System\Logon	Always wait for the network at computer startup and logon	Включен
Конфигурация компьютера\ Административные шаблоны\ System\Scripts	Run startup scripts asynchronously	Отключен

Табл. 11. Параметры для ОС Windows 2000 Server

Раздел	Параметр	Значение
Конфигурация компьютера\ Административные шаблоны\ System\Logon	Run startup scripts asynchronously	Отключен
Конфигурация компьютера\ Административные шаблоны\ System\Group Policy	Apply Group Policy for computers asynchronously during startup	Отключен

Некоторые рекомендации по обеспечению безопасности в ИС

Ниже приведены некоторые рекомендации Microsoft по обеспечению информационной безопасности в информационной системе (ИС) предприятия:

- Для предотвращения атак домена переименуйте или отключите встроенную учетную запись администратора (а также учетную запись гостя) в каждом домене.
- Держите все контроллеры домена в закрытой комнате для обеспечения физической безопасности.
- Для обеспечения дополнительной защиты схемы Active Directory контролируйте состав группы "Администраторы схемы" и добавляйте пользователей в эту группу только при необходимости.
- Ограничьте для пользователей, групп и компьютеров доступ к общим ресурсам и к параметрам фильтра групповой политики.
- Избегайте отключения подписывания и шифрования трафика LDAP для средств администрирования Active Directory.
- Некоторые права пользователей по умолчанию, присвоенные определенным группам по умолчанию, позволяют членам этих групп получить дополнительные, в том числе административные, права в домене. Поэтому организация должна в равной степени доверять всем сотрудникам, являющимся членами групп "Администраторы предприятия", "Администраторы домена", "Операторы учета", "Операторы сервера", "Опытные пользователи", "Операторы печати" и "Операторы архива".

Источник: Microsoft TechNet.

О восстановлении регистрации сервера безопасности в AD

В результате восстановления регистрации сервера безопасности в AD все его настройки, включая лицензионную информацию, возвращаются в значения по умолчанию. При возвращении настроек сервера в значения по умолчанию происходит восстановление целостности параметров сервера и удаляются серийные номера, хранимые на сервере.

В результате удаления серийных номеров подчиненные серверу безопасности компьютеры становятся свободными и перестают управляться системой Secret Net 6, а при загрузке сервера появляется сообщение о нарушении лицензионной политики.

Для восстановления подчинения компьютеров серверу безопасности:

1. Запустите программу конфигурирования и выполните следующие действия:
   - введите для данного сервера безопасности все серийные номера, которые должны храниться на нем;
   - добавьте свободные компьютеры (ранее подчиненные данному серверу безопасности) в программу конфигурирования и подчините их серверу.
2. Перезагрузите компьютер с сервером безопасности.
3. Вернитесь к программе конфигурирования и проверьте значения параметров сервера безопасности, при необходимости — откорректируйте их.
4. Запустите программу мониторинга и убедитесь в работоспособности сервера безопасности.

Для восстановления регистрации сервера безопасности в AD

1. В процедуре переустановки сервера безопасности при выполнении действия **6** (см. стр. 24) в диалоге "Регистрация в Active Directory" установите отметку в поле "восстановить регистрацию компонентов программы в Active Directory" и нажмите кнопку "Далее >".

   На экране появится диалог "Модификация Active Directory".
2. Укажите учетные данные пользователя с правами администратора домена и нажмите кнопку "Далее >".

   Пояснение. Если текущий пользователь имеет права на запись в AD — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   На экране появится диалог "Подчинение сервера".

   Пояснение. Диалог не появится, если переустанавливается единственный в домене сервер безопасности. В этом случае пропустите действие 3.
3. Выполните следующие действия:
   - Определите подчиненность сервера безопасности:
     - если требуется иерархию подчиненности серверов безопасности установить позже — выберите пункт "не подчинять этот сервер другому серверу";
     - если требуется установить подчиненность сервера безопасности — выберите пункт "подчинить этот сервер другому серверу и настроить параметры подключения" и из раскрывающихся списков выберите имя хоста сервера, которому будет подчинен устанавливаемый, и скоростные параметры вашей ЛВС.
   - Нажмите кнопку "Далее >".

   На экране появится диалог "Название организации".
4. Укажите названия организации и подразделения, которое будет обслуживать устанавливаемый сервер, и нажмите кнопку "Далее >".

   На экране появится сообщение: "Подходящий сертификат уже установлен".
5. Примите решение о замене сертификата, для чего нажмите одну из кнопок "Да" или "Нет".

На экране появится диалог: "Готова к исправлению программы".

6. Нажмите кнопку "Установить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса.

   После успешной установки и настройки компонентов на экране появится диалог "Программа установки завершена".

7. Нажмите кнопку "Готово" и перезагрузите компьютер.

Терминологический справочник

A	
AD	Active Directory — служба каталога для операционных систем MS Windows 2000 Server и выше. Active Directory Schema (схема Active Directory или схема каталога AD) — набор правил, описывающих структуру каталога (классы объектов домена и их атрибуты). Схема каталога AD гарантирует, что все добавления или изменения каталога соответствуют правилам
I	
IIS	Internet Information Services — компонент Windows
L	
LDAP	Lightweight Directory Access Protocol — протокол, работающий в домене поверх TCP/IP и обеспечивающий доступ к данным в AD
O	
OID	Идентификатор объекта (Object Identifier)
S	
SID	Идентификатор безопасности (Security Identifier)
А	
Администратор безопасности	Лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
Аутентификация	Проверка регистрационной информации пользователя
Г	
Глобальный каталог	Глобальный каталог (Global Catalog — GC) хранит полную копию всех объектов AD для того домена, в который входит сервер GC, и частичную копию объектов других доменов, образующих лес (хранятся только те свойства объектов, которые представляют интерес с точки зрения «масштабов» леса). С помощью оснастки Active Directory Schema администраторы могут указывать свои атрибуты (свойства объектов) для хранения в GC
Ж	
Журнал регистрации событий	Хранилище с информацией о событиях, зарегистрированных в системе защиты, например, попытках входа в систему
М	
Модификатор AD	Модификатор AD (или Модификатор схемы) — программа, которая вносит в схему каталога Active Directory классы и атрибуты, описывающие объекты Secret Net 6. Без модификации схемы AD невозможна установка Secret Net 6 в информационной системе

С

Средства управления Программы оперативного управления, к которым относятся программы "Журналы" (в централизованном режиме работы), "Монитор" и "Консоль управления". Установка всех трех программ происходит одновременно при установке компонента "Secret Net 6 — Средства управления"

Документация

1	Средство защиты информации Secret Net 6. Принципы построения. Руководство администратора	RU.88338853.501410. 007 91 1
2	Средство защиты информации Secret Net 6. Установка, обновление и удаление. Руководство администратора	RU.88338853.501410. 007 91 2
3	Средство защиты информации Secret Net 6. Управление. Основные механизмы защиты. Руководство администратора	RU.88338853.501410. 007 91 3
4	Средство защиты информации Secret Net 6. Управление. Полномочное управление доступом и контроль печати. Руководство администратора	RU.88338853.501410. 007 91 4
5	Средство защиты информации Secret Net 6. Аудит. Руководство администратора	RU.88338853.501410. 007 91 5
6	Средство защиты информации Secret Net 6. Мониторинг и оперативное управление. Руководство администратора	RU.88338853.501410. 007 91 6
7	Средство защиты информации Secret Net 6. Конфигурирование. Руководство администратора	RU.88338853.501410. 007 91 7
8	Средство защиты информации Secret Net 6. Аппаратные средства. Руководство администратора	RU.88338853.501410. 007 91 8
9	Средство защиты информации Secret Net 6. Руководство пользователя	RU.88338853.501410. 007 92
10	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство администратора	УВАЛ. 00300-58-01 91
11	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство пользователя	УВАЛ. 00300-58-01 92
12	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора	RU.40308570.501410. 001 91
13	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство пользователя	RU.40308570.501410. 001 92